

REMARKS/ARGUMENTS

Claims 1-27 stand rejected in the outstanding Official Action. Claims 1-10, 13-15, 17-20, 22-24 and 27 have been amended and therefore claims 1-27 remain in this application.

The Examiner, in the first section on page 2, requires new formal drawings. While Applicant traverses the requirement of formal drawings in a particular format, new formal drawings are enclosed herewith, thereby obviating any further objection thereto.

Claims 1-9 stand rejected under 35 USC §101 as being directed to non-statutory subject matter. While Applicant respectfully traverses the requirement of any particular verbiage in order to identify the claimed invention, Applicant has adopted the Examiner's suggested wording of "a program stored on a computer-readable medium" and has amended claims 1-9 accordingly. Therefore, any further rejection of claims 1-9 under 35 USC §101 is respectfully traversed.

Claims 1-3, 6-12, 15-21 and 24-27 stand rejected under 35 USC §102(e) as anticipated by Schertz (U.S. 2003/0084322). Applicant's independent claims 1, 10 and 19 each recite either structure, method step or logic for accomplishing two functions. First, they all recite detecting from the plurality of log data messages "**a pattern of malware detection across said plurality of network connected computers.**" Second, in response to the detecting of a pattern, there is the performance of "**at least one predetermined anti-malware action.**" In order to support a rejection of the claims as being anticipated by §102(e), it is incumbent upon the Examiner to establish how or where the Schertz prior art reference shows both features of Applicant's independent claims.

The Schertz reference discloses an intrusion detection and anti-virus system for operation on a network. An intrusion protection system management computer 85 is provided, as

discussed in paragraph 22, to receive alerts from other nodes within the system and “to facilitate configuration and management of the intrusion protection system components.” While the Examiner specifically references paragraph 30 of Schertz, this appears to relate to assembling higher level data from fragments of network traffic such that signatures of unwanted activity can be identified within those assembled collections which would otherwise not be identifiable.

With respect to the applicant’s claimed feature of detecting “a pattern of malware detection,” the Examiner points to three portions of the Schertz reference, i.e., page 4, paragraph 30, lines 9-21, page 3, paragraph 21, lines 10-18 and page 3, paragraph 23, lines 12-18. Nowhere in any of these cited passages from the Schertz reference is there disclosed anything relating to “a pattern,” let alone detecting a “pattern of malware detection across said plurality of network connected computers.” In fact, the citation on page 4, paragraph 30 does not even include logging of data messages from which Applicant’s invention detects the pattern. Accordingly, since Schertz contains no disclosure of this feature of independent claims 1, 10 and 19, it cannot anticipate the subject matter of Applicant’s claims.

Turning to the second feature of applicant’s independent claims, obviously since there is no pattern detection, Schertz cannot teach performing any action in response to the pattern detection. Again, while the Examiner cites similar portions of the Schertz reference (page 4, paragraph 30, lines 16-21 and page 3, paragraph 20, lines 14-25), a careful review of those cited portions does not reveal that any action is taken in response to detecting “a pattern of malware detection across said plurality of network connected computers.” As a result, the failure of Schertz to disclose this second feature of Applicant’s independent claims 1, 10 and 19 again disqualifies it as prior art under 35 USC §102.

Should the Examiner be of the opinion that Schertz contains any disclosure of the two mentioned features in Applicant's independent claims, he is respectfully requested to point out exactly where that occurs -- particularly, any indication that Schertz looks at messages to detect a "pattern of malware detection." Again, this is not the detection of a virus, but rather the detection of a "pattern of malware detection" across the network of connected computers. Such is simply not suggested, let alone disclosed in the Schertz reference. In view of the above, Schertz clearly fails to anticipate claims 1, 10 and 19 and claims dependent thereon under 35 USC §102(e) and any further rejection thereunder is respectfully traversed.

Claims 4, 13 and 22 stand rejected under 35 USC §103 as unpatentable over Schertz in view of Schnurer (U.S. Patent 5,842,002). Inasmuch as claims 4, 13 and 22 ultimately depend from independent claims 1, 10 and 19, respectively, the above comments distinguishing claims 1, 10 and 19 from the Schertz reference are herein incorporated by reference. The Examiner's admission that "Schertz do [sic] not explicitly teach updating of malware definition data" is very much appreciated. While the Examiner suggests that Schnurer teaches a computer program product/method/apparatus in which anti-malware actions include an update of malware definition data, there is no indication that Schnurer teaches the missing structures set out in Applicant's claims from the Schertz reference, i.e., detecting "a pattern of malware detection" and then in response to said detection performing "predetermined anti-malware actions."

As a result, because neither Schertz nor Schnurer teach the subject matter of Applicant's independent claims 1, 10 and 19, dependent claims 4, 13 and 22 cannot be considered obvious in view of the Schertz/Schnurer combination and any further rejection thereunder is respectfully traversed.

Claims 5, 14 and 23 stand rejected under 35 USC §103 as unpatentable over Schertz in view of Chen (U.S. Patent 5,832,208). It is noted that claims 5, 14 and 23 ultimately depend from independent claims 1, 10 and 19, respectively. Accordingly, the above comments distinguishing independent claims 1, 10 and 19 from the Schertz reference are herein incorporated by reference. Again, the Examiner's admission that Schertz "does not explicitly teach altering the scanner setting when malware is detected" is very much appreciated. It is noted that the Examiner does not allege or suggest that the Chen reference teaches missing claimed elements from the Schertz reference, i.e., detecting "a pattern of malware detection" and then in response to such detection performing "at least one predetermined anti-malware action."

Because neither Schertz nor Chen disclose the features of Applicant's independent claims 1, 10 and 19, they cannot render obvious the subject matter of dependent claims 5, 14 and 23 and any further rejection under 35 USC §103 is respectfully traversed.

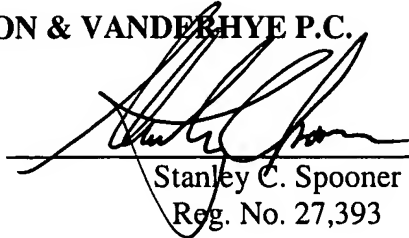
Having responded to all objections and rejections set forth in the outstanding Official Action, it is submitted that pending claims 1-27 are in condition for allowance and notice to that effect is respectfully solicited. In the event the Examiner is of the opinion that a brief telephone or personal interview will facilitate allowance of one or more of the above claims, he is respectfully requested to contact Applicant's undersigned representative.

ACKROYD
Appl. No. 10/036,521
June 2, 2005

Respectfully submitted,

NIXON & VANDERHYTE P.C.

By:



Stanley C. Spooner
Reg. No. 27,393

SCS:kmm
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

ACKROYD
Appl. No. 10/036,521
June 2, 2005

AMENDMENTS TO THE DRAWINGS

Please substitute the attached formal drawings for the originally filed formal drawings.